Deliberation no. 2020-050 of 30 April 2020 on the adoption of the requirements for accreditation of monitoring bodies in charge of the monitoring of compliance with a code of conduct

Courtesy translation - in the event of any inconsistencies between the French adopted version and this English courtesy translation, please note that the French version shall prevail and have legal validity.

The Commission nationale de l'Informatique et des Libertés (French Data Protection Authority),

Having regard to the Council of Europe Convention n°108 for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, particularly its articles 41 et 57.1.p);

Having regard to Act no. 78-17 of 6 January 1978, amended, on information technology, data files and civil liberties;

Having regard to Decree no. 2019-536 of 29 May 2019, amended, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to European Data Protection Board (EDPB) Guidelines on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 adopted on 4 June 2019;

Having heard the report of Ms Anne DEBET, commissioner, and the observations of Ms Nacima BELKACEM, government commissioner.

Makes the following observations:

1. Article 41 of the General Data Protection Regulation (GDPR) provides that compliance monitoring of approved codes of conduct may be carried out by a monitoring body which has an appropriate level of expertise in relation to the subject-matter of the code. Such bodies must be accredited for that purpose by the competent supervisory authority.

2. Article 57.1.p) of the GDPR provides that each supervisory authority shall draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41.

3. Article 41.3 of the GDPR states that accreditation projects set out by each national supervisory authority shall be submitted to the consistency mechanism and communicated to the European Data Protection Board (EDPB).

4. On 3 October 2019, a draft accreditation requirement was adopted by the Commission and submitted to the EDPB on 18 October 2019. The EDPB adopted an opinion regarding this draft on 28 January 2020, which was notified to the Commission on 4 February 2020.

5. This deliberation sets out the criteria for accreditation requirements for code of conduct monitoring bodies, as referred to in Article 41 of Regulation (EU) 2016/679.

Decides:

To adopt the accreditation requirements for code of conduct monitoring bodies attached to this deliberation.

The accreditation term will be initially set at five years, without prejudice to the CNIL's ability to exercise its powers at any time as regards the monitoring body's obligations.

The procedure to initially request and subsequently renew accreditation is set out by the CNIL's internal rules of procedure. Renewal requires a reassessment of the monitoring body's eligibility, which may result in a favourable outcome or a refusal.

This decision will be published in the Official Journal of the French Republic.

The Chair

Marie-Laure Denis

APPENDIX 1: accreditation requirements for codes of conduct monitoring bodies

General remarks:

Article 40.4 of the GDPR provides that codes of conduct shall contain mechanisms enabling the body referred to in Article 41 of the Regulation to monitor compliance with said codes. Such bodies may be internal or external (as *ad hoc* committees). The requirements listed below shall apply to the monitoring body, whether internal or external.

"The supervisory authority" referred to in the requirements below is the French data protection authority (hereinafter the CNIL).

Requirements
1. General requirements
Explanatory note: These requirements aim to set out a general framework for the monitoring body's activities. They also include the guarantees that it must provide to demonstrate proper management of its activities and its financial and material independence.
1.1 The monitoring body shall implement an approach aiming to ensure that all processing operations it performs for its monitoring tasks are compliant with the GDPR.
1.2 The monitoring body shall demonstrate that all appropriate human, financial and material resources in proportion with the code of conduct's scope are used. Such resources are adapted to the number and size of code members and to the level of complexity or risk of the processing carried out by code members.
1.3 The monitoring body's obligations and the core elements of its function are set out in the code of conduct.
1.4 The monitoring body shall ensure that the documents relating to the performance of its duties (documents provided, audit plan, audit evidence, audit reports, etc.) are stored in a way that maintains their confidentiality or are definitely and securely destroyed if they are no longer of when the monitoring tasks are over (subject to other legal obligations or legitimate grounds).
1.5 The monitoring body shall ensure when performing its tasks; that it complies with the security measures provided by the code member. These security measures shall not prevent the monitoring body from performing its tasks.
2. Requirements relating to the monitoring body's independence
Explanatory note: A monitoring body's independence is ensured by implementing formal rules and procedures which govern its appointment, its mandate and its functioning. When requesting accreditation from the supervisory authority, the monitoring body must demonstrate its functional, material and decision-making independence. Compliance with each requirement will be assessed in light of the supporting documents provided.

The requirements and examples listed below shall apply to the monitoring body, whether internal or external.

2.1 The monitoring body shall demonstrate its independence, particularly with regards to the code owner, the code members and members of the specific sector of the code.

2.2 The monitoring body shall demonstrate its functional independence with regards to the code owner and code members when performing its tasks and exercising its powers.

The monitoring body must have the necessary human and technical resources to efficiently perform its tasks. The monitoring body shall demonstrate that it is able to fully perform its monitoring duties, taking into consideration the specific sector and the risks associated with the processing activities to which the code of conduct applies.

2.3 The monitoring body shall demonstrate its financial independence by providing evidence of sufficient financial resources and financial viability to perform its duties.

The monitoring body shall demonstrate that the rules relating to its financing prevent any risk of compromising its independence or the performance of its tasks, including from a code member.

2.4 The monitoring body shall demonstrate its independence during the decision-making process, including the choice of its personnel entrusted with monitoring duties.

2.5 The monitoring body shall demonstrate that it is solely responsible for decision-making when performing its monitoring tasks.

Without prejudice to the supervisory authority's tasks and powers, decisions made by the monitoring body relating to its functions are not submitted to another body for approval, including to the code owner.

3. Requirements relating to the absence of conflicts of interest

Explanatory note:

The absence of conflicts of interest is ensured by implementing measures and procedures aiming to prevent such situations.

3.1 The monitoring body shall remain free from any direct or indirect external influence.

It shall not seek nor take instructions from any person, organisation or association.

3.2 The monitoring body shall be able to identify any situation likely to create a conflict of interest (due to its personnel, its organisation, its procedures, its subcontractors, etc.)

3.3 The monitoring body shall implement procedures and measures to avoid conflicts of interest so as to refrain from any action incompatible with its duties and functions.

The monitoring body must set out a procedure to handle any situation likely to create a conflict of interest.

3.4 The monitoring body must have its own personnel, selected by itself or by a service provider that is independent from the code.

4. Requirements relating to the monitoring body's expertise

Explanatory note:

Each request for accreditation is assessed *in concreto*, also taking into account the specific expertise requirements set out by the code of conduct.

Expertise requirements are set out taking into account various factors such as the specific sector of the code of conduct, the size of this sector, the number of code members, the risks tied to the processing activities and the different interests at stake.

4.1 Requirements relating to management personnel in charge of the decision-making process

4.1.1 The monitoring body shall demonstrate that it has the necessary expertise to properly perform the monitoring activities under the code of conduct.

4.1.2 The monitoring body shall demonstrate that the personnel in charge of the decision-making has in-depth knowledge on and experience in the topics and issues relating to data protection and in the specific sector the code of conduct addresses, as well as in the performance of monitoring tasks.

Such expertise is not necessarily concentrated by one single individual.

4.2 Requirements relating to personnel performing monitoring tasks

4.2.1 The personnel shall have undergone training on audit methods (audit principles, audit procedures and techniques, documents relating to audits, regulations and other applicable requirements, etc.).

4.2.2 The personnel shall have taken part in at least two full audits, from their preparation to the final conclusions, in the last three years.

4.2.3 The personnel shall be able to benefit from continuing training.

4.2.4 The personnel shall have the necessary level of expertise as regards the processing activities referred to in the code and in-depth knowledge on the data protection topics relating to the specific sector of the code.

4.2.5 The personnel shall have undergone a specific training on personal data protection.

4.2.6 The personnel with a legal profile shall hold *a minima* a first year Master's degree or an equivalent degree in the legal field.

4.2.7 The personnel with a legal profile shall have at least two years of professional experience in the field of personal data protection (e.g. consulting, litigation, etc.).

4.2.8 The personnel with a technical profile shall hold *a minima* a bachelor's degree or an equivalent degree in the field of computer sciences, information systems or cybersecurity.

4.2.9 The personnel with a technical profile have undergone at least a two days' training on relevant standards for information system security management (regulations, standards, methods, best practices, risk management, etc.).

4.2.10 The personnel with a technical profile shall have at least two years' experience in the field of information system security.

5. Requirements relating to the monitoring body's procedures

Explanatory note:

These requirements aim to guarantee that the monitoring tasks and duties carried out by the monitoring body are regular, complete and transparent for the member of the code of conduct.

The monitoring procedure can be shaped in different ways such as random or unannounced audits, annual inspections, regular reporting and the use of questionnaires.

The monitoring procedure implemented by the monitoring body is in accordance with the framework given by the code of conduct.

5.1 The monitoring body must demonstrate that the audit procedure sets out which expertise is necessary to perform its tasks and guarantees that the personnel possesses the necessary expertise to conduct the monitoring tasks.

5.2 The monitoring body shall demonstrate that the monitoring procedure includes a commitment from the personnel to comply with the rules pertaining to ethics, independence, unbiased presentation of results and the use of a methodical approach.

5.3 The monitoring body shall demonstrate that the procedure provides for regular controls, carried out in an independent manner and which enable:

- an assessment of data controllers' and/or processors' eligibility to adhere to the code of conduct,
- a monitoring of the compliance with the code after adherence, and
- a review of the proper functioning of the code's operation.

5.4 The monitoring body shall demonstrate that it has put in place a monitoring programme which takes into account such elements as the complexity of processing operations and the risks associated with the data processing, the number of code members, the code's geographic scope and the received complaints.

5.5 The monitoring body shall demonstrate that the monitoring procedure ensures the integrity and traceability of evidence when collecting necessary information.

5.6 The monitoring body shall demonstrate that the monitoring results and conclusions are presented and explained to audited code members within a reasonable period of time.

In the context of a monitoring, written or oral comments made by a code member upon receipt of findings and conclusions are listed in the report.

6. Requirements relating to the processing of complaints

Explanatory note:

The monitoring body implements procedures to ensure the impartial and objective processing of complaints pertaining to code violations or the manner in which the code is applied by a code member. These procedures are transparent and public to all.

The handling complaint procedure established by the monitoring body handles complaints from a code member or from any person who can demonstrate a legitimate interest. This process should be sufficiently resourced and personnel should demonstrate sufficient knowledge and impartiality.

This procedure is also based on the applicable code of conduct.

6.1 The monitoring body shall establish a procedure to receive, manage and process complaints. The monitoring body shall demonstrate that this procedure is unbiased and transparent.

6.2 This procedure shall be accessible and easily understood by all, including data subjects and code members.

6.3 The monitoring body ensures that all complaints are processed and provides the complainant with reports on the procedure's progress or its results within a reasonable period of time, e.g. three months, as from receipt of the complaint.

The period required for resolution of the complaint may be extended for a reasonable period where necessary, taking account of the complexity of the complaint. The monitoring body shall inform the complainant of such an extension within three months as from receipt of the complaint and specify the reasons for extending the deadline.

6.4 The monitoring body shall keep a record of the processing of all complaints received. The monitoring body keeps this record readily available to the supervisory authority, which may access it at any time.

6.5 The monitoring body shall make its decisions, or general information thereof, publicly available, pursuant to its complaints handling procedure.

Such general information may include, but is not limited to, general statistical data on the number and type of complaints/infringements received and the resolutions/corrective measures issued. Such general information must include information relating to the sanctions having resulted in the suspension or exclusion of a code member.

7. Requirements relating to information of the supervisory authority

Explanatory note:

These requirements list the information that a monitory body must provide to the supervisory authority on a regular basis.

7.1 The monitoring body shall compile in a single document the summaries of all of the actions undertaken. The document is at the disposal of the supervisory authority which can access it at any time.

7.2 The monitoring body shall inform the supervisory authority, without undue delay and in writing, of any substantial change (particularly relating to structure or organisation) likely to call into question its independence, expertise and the absence of any conflict of interests.

7.3 The monitoring body shall inform the supervisory authority, in writing, when a binding measure is taken against a code member. This notice includes the reasons justifying the measure.

The frequency of communication is based on several criteria, including the seriousness of the infringement and of the adopted measure.

7.4 The monitoring body shall inform the supervisory authority, without undue delay and in writing, as soon as a code member is suspended. This notice includes the reasons justifying the measure.

7.5 The monitoring body shall inform the supervisory authority, without undue delay and in writing, as soon as a code member is excluded from the code of conduct. This notice includes the reasons justifying the measure.

8. Requirements relating to review mechanisms

Explanatory note:

The code owner may decide to change or extend the code's scope and/or its content. In that case, monitoring bodies are involved in this process: they play a key role by contributing to the update of the code of conduct pursuant to the review mechanisms set out by the code of conduct.

8.1 The monitoring body participates in the review and/or changes to the code decided by the code owner.
8.2 The monitoring body must set out procedures to implement and monitor the application of the changes decided by the code owner.
8.3 The monitoring body also provides the code owner with a periodical report on the proper functioning of the code's operation.
9. Requirements relating to legal status
9.1 Requirements relating to the monitoring body
9.1.1 The monitoring body is established in the European Union.
9.1.2 The monitoring body remains responsible to the supervisory authority, for all tasks and decisions relating to its duties.
9.1.3 The monitoring body has sufficient financial, human and material resources and has procedures ensuring the continuity of its monitoring duties for the duration of its accreditation.
9.2 Requirements relating to the management of subcontracting
Explanatory note: The aim of these requirements is to ensure compliance with this accreditation requirements when the monitoring body subcontracts parts of its tasks.
9.2.1 The monitoring body shall establish a contract or any other legal act under European Union law binding on the subcontractor with regard to the monitoring body in such a way that all subcontracted tasks will meet the requirements of the GDPR. Recourse to subcontracting does not result in the delegation of responsibilities: in any case, the monitoring body remains responsible for monitoring compliance with the code of conduct to the supervisory authority.
9.2.2 The monitoring body ensures that all subcontractors meet the requirements set out by this accreditation requirements document, notably as regards independence, absence of conflict of interest and expertise.
9.2.3 The monitoring body includes a specific clause in the contract signed with subcontractors to ensure the confidentiality of personal data that may, where applicable, be disclosed to the subcontractor during the monitoring tasks.

10. Requirements relating to the sanctions and corrective measures decided by the monitoring body
10.1 The monitoring body applies the corrective measures and sanctions set out in the code of conduct.
10.2 When it enforces the application of corrective measures or issues sanctions in accordance with the code of conduct, the monitoring body shall ensure that the code member's rights are respected.